REMARKS

Claims 1, 4, 6-12, 15, 23 and 26 are pending in this application. All of the pending claims were rejected. Claims 1, 12 and 23 are currently amended. Reconsideration is requested.

Claim 23 was rejected under 35 U.S.C. 101 as being directed to software *per se*. Claim 23 as currently amended recites physical memory circuitry and a microprocessor. Support for these limitations is in the specification at page 22, line 29 through page 23, line 2. Withdrawal of the rejection is therefore requested.

Claims 1, 4, 6-12, 15, 23 and 26 were rejected for obviousness-type double patenting based on co-pending US 10/661,903. A terminal disclaimer is submitted with this response to overcome the rejection.

Claims 1, 4, 6-12, 15, 23 and 26 were rejected under 35 U.S.C. 103(a) based on US 2002/0154635 (Liu) in combination with US 6,970,941 (Caronni) and US 6,185,650 (Shimbo). The reasons for the rejections are unchanged from the previous office action. The examiner provides no response to the arguments, and does not discuss the new limitations. Applicant is therefore placing the claims in better condition for appeal by replacing language which might be interpreted as making some of the limitations optional, and adding more emphasis on the distinguishing feature that point-to-point security associations are used for group security when communications are not common to the group. Group security associations are known for communications that are shared between a group of more than two members, e.g., multicast. However, group security associations are neither known for, nor designed for, communications between only two members. Rather, point-to-point security associations are used for communications between only two members. Although point-to-point security associations provide security from other members, the amount of data that must be stored to support N point-

to-point connections increases at a rate of N^2-1, which causes a scalability problem. The presently claimed invention provides scalable point-to-point security by utilizing group security associations for point-to-point communications, i.e., group members that are neither senders nor receivers share the same group security association with the sender and receiver.

None of the cited references teach use of group security associations for point-to-point security. Further, the feature is counter-intuitive because it requires that members which are neither senders nor receivers have the group security association used for communication by other devices. The purpose of point-to-point security is to avoid sharing security associations with devices which are neither senders nor receivers. Therefore, any attempted combination of point-to-point and group security references is contradictory, unless those references include a specific teaching that the level of security normally associated with point-to-point security should be reduced in order to improve scalability.

It should be noted that "group security association" is a term of art, and the examiner's interpretation of that term is in disagreement with the understanding of those of ordinary skill in the art. The Examiner cites Caronni at column 7, lines 5-33; column 3, lines 17-21; and column 11, lines 37-43 as teaching the limitation of transforming the packet according to a group security association associated with the private network as recited in the independent claims. The Examiner explains that "the mappings of the internal/private address, known as node ID, which is considered as a part of the group security association … the security association (SA) is related to Authentication Header (AH) … ." As described in the specification of this application at page 11, line 12 through page 12, line 5, and widely understood in the art, a Group Security Association (GSA) is a bundling of SAs that together define how a group securely communicates, e.g., selectors, properties, cryptographic policy and keys. Applicant submits that

the Examiner's assertion that a mapping between internal and external addresses is analogous to a GSA is fundamentally flawed because such a mapping is neither covered by the description in the specification nor capable of providing any practical measure of security for communications. The cited passage at column 7 describes such an address mapping, and there is no indication in Caronni that the external address is secure or used for a group. Indeed, there is no indication that the mapping is anything more than the result of address resolution for routing purposes. Caronni describes providing security elsewhere, but only point-to-point security techniques which suffer the scalability problem discussed above. For example, the cited passage at column 3 describes "secure communications between nodes," rather than secure communications between all nodes associated with a group using the same GSA. The cited passage at column 11 is unrelated to security. The claims further distinguish the cited combination because Caronni fails to describe transforming the packet according to a group security association associated with the private network.

Claims 4, 6-11, 15, and 26 are dependent claims which further define the invention, and which are allowable for the same reasons as their respective base claims.

Applicants have made a diligent effort to place the claims in condition for allowance. Should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone Applicants' Attorney at the number listed below so that such issues may be resolved as expeditiously as possible. For these reasons, and in view of the above amendments, this application is now considered to be in condition for allowance and such action is earnestly solicited.

Respectfully Submitted,

October 20, 2008
Date

/Holmes W. Anderson/
Holmes W. Anderson, Reg. No. 37272
Attorney/Agent for Applicant(s)
Anderson Gorecki & Manaras LLP
33 Nagog Park
Acton, MA 01720
(978) 264-4001

Docket No. 120-306
Dd: 8/21/2008